LWAPP 업그레이드 도구 문제 해결 팁

목차

소개

이 문서에서는 자동 액세스 포인트(AP)를 경량 모드로 업그레이드하기 위해 업그레이드 도구를 사용할 때 발생할 수 있는 몇 가지 주요 문제에 대해 설명합니다.이 문서에서는 이러한 문제를 해결하는 방법에 대한 정보도 제공합니다.

사전 요구 사항

요구 사항

업그레이드를 수행하려면 AP에서 Cisco IOS® Software Release 12.3(7)JA 이상을 실행해야 합니다.

Cisco 컨트롤러는 최소 소프트웨어 버전 3.1을 실행해야 합니다.

Cisco WCS(Wireless Control System)는 최소 버전 3.1을 실행해야 합니다.

업그레이드 유틸리티는 Windows 2000 및 Windows XP 플랫폼에서 지원됩니다.이러한 Windows 운영 체제 버전 중 하나를 사용해야 합니다.

사용되는 구성 요소

이 문서의 정보는 이러한 액세스 포인트 및 무선 LAN 컨트롤러를 기반으로 합니다.

이 마이그레이션을 지원하는 AP는 다음과 같습니다.

- 모든 1121G 액세스 포인트
- 모든 1130AG 액세스 포인트
- 모든 1240AG 액세스 포인트
- 모든 1250 시리즈 액세스 포인트
- 모든 IOS 기반 1200 Series 모듈형 액세스 포인트(1200/1220 Cisco IOS Software Upgrade, 1210 및 1230 AP) 플랫폼의 경우 라디오에 따라 다릅니다.802.11G, MP21G 및 MP31G가 지원되는 경우802.11A, RM21A 및 RM22A가 지원되는 경우1200 Series 액세스 포인트는 지원되는 라디오 조합으로 업그레이드할 수 있습니다.G 전용, A 전용 또는 G 및 A 둘 다. 이중 무선 장치가 포함된 액세스 포인트의 경우 두 무선 통신 중 하나가 LWAPP에서 지원하는 무선 통신 장치인 경우 업그레이드 도구는 업그레이드를 계속 수행합니다.툴은 지원되지 않는 무선을 나타내는 경고 메시지를 세부 로그에 추가합니다.
- 모든 1310 AG 액세스 포인트
- Cisco C3201 WMIC(Wireless Mobile Interface Card)**참고:** 2세대 802.11a 무선 장치에는 두 개의 부품 번호가 있습니다.

업그레이드를 수행하려면 액세스 포인트가 Cisco IOS Release 12.3(7)JA 이상을 실행해야 합니다.

Cisco C3201WMIC의 경우, 업그레이드를 수행하려면 액세스 포인트가 Cisco IOS 릴리스 12.3(8)JK 이상을 실행해야 합니다.

이러한 Cisco 무선 LAN 컨트롤러는 경량형 모드로 업그레이드된 자동 액세스 포인트를 지원합니다.

- 2000 시리즈 컨트롤러
- 2100 시리즈 컨트롤러
- 4400 시리즈 컨트롤러
- Cisco Catalyst 6500 Series 스위치용 Cisco Wireless Services Module(WiSM)
- Cisco 28/37/38xx Series Integrated Services Router 내의 컨트롤러 네트워크 모듈
- Catalyst 3750G Integrated Wireless LAN Controller Switch

Cisco 컨트롤러는 최소 소프트웨어 버전 3.1을 실행해야 합니다.

Cisco WCS(Wireless Control System)는 최소 버전 3.1을 실행해야 합니다. 업그레이드 유틸리티는 Windows 2000 및 Windows XP 플랫폼에서 지원됩니다.

Cisco Software Downloads 페이지에서 최신 버전의 업그레이드 유틸리티를 다운로드할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

업그레이드 프로세스 - 개요

사용자는 액세스 포인트 목록과 해당 자격 증명이 포함된 입력 파일을 수락하는 업그레이드 유틸리티를 실행합니다.이 유틸리티는 일련의 Cisco IOS 명령을 입력하여 업그레이드를 위한 액세스 포인트를 준비합니다. 여기에는 자체 서명 인증서를 생성하는 명령이 포함됩니다.또한 이 유틸리티는 컨트롤러에 연결하여 특정 자체 서명 인증서 액세스 포인트의 권한 부여를 허용하도록 디바이스를 프로그래밍합니다.그런 다음 Cisco IOS Software Release 12.3(11)JX1을 액세스 포인트에 로드하여 컨트롤러에 조인할 수 있습니다.액세스 포인트가 컨트롤러에 연결되면 컨트롤러에서 완전한 Cisco IOS 버전을 다운로드합니다.업그레이드 유틸리티는 WCS 관리 소프트웨어로 가져올 수 있는 액세스 포인트 목록과 해당 자체 서명 인증서 키 해시 값을 포함하는 출력 파일을 생성합니다.그런 다음 WCS는 이 정보를 네트워크의 다른 컨트롤러로 보낼 수 있습니다.

자세한 내용은 자동 Cisco Aironet 액세스 포인트를 경량형 모드로 업그레이드의 업그레이드 절차 섹션을 참조하십시오.

업그레이드 도구 - 기본 작업

이 업그레이드 도구는 AP가 이 업그레이드에 호환될 경우 자동 AP를 경량 모드로 업그레이드하는 데 사용됩니다.업그레이드 도구는 자동 모드에서 경량 모드로 업그레이드하는 데 필요한 기본 작업을 수행합니다.이러한 작업은 다음과 같습니다.

- Basic condition checking(기본 조건 검사) - AP가 지원되는 AP인지, 최소 소프트웨어 버전을 실행하는지 여부 및 라디오 유형이 지원되는지 여부를 확인합니다.
- AP가 루트로 구성되었는지 확인합니다.
- 변환을 위한 자동 AP 준비 - PKI(Public Key Infrastructure) 컨피그레이션 및 인증서 계층 구조를 추가하여 Cisco 컨트롤러에 대한 AP 인증이 발생할 수 있으며 AP에 대해 자체 서명 인증서(SSC)가 생성될 수 있습니다.AP에 MIC(Manufacturing-Installed Certificate)가 있는 경우 SSC는 사용되지 않습니다.
- 12.3(11)JX1 또는 12.3(7)JX와 같이 AP가 컨트롤러에 조인할 수 있는 자동-경량 모드 업그레이드 이미지를 다운로드합니다.다운로드가 성공하면 AP가 리부팅됩니다.
- AP MAC 주소, 인증서 유형 및 보안 키 해시로 구성된 출력 파일을 생성하고 컨트롤러를 자동으로 업데이트합니다.출력 파일을 WCS로 가져와서 다른 컨트롤러로 내보낼 수 있습니다.

중요 참고 사항

이 유틸리티를 사용하기 전에 다음 중요한 사항을 고려하십시오.

- 이 도구로 변환된 액세스 포인트는 40xx, 41xx 또는 3500 컨트롤러에 연결되지 않습니다.
- 802.11b 전용 또는 1세대 802.11a 무선 장치로 액세스 포인트를 업그레이드할 수 없습니다.
- 변환 및 재부팅 후 액세스 포인트의 고정 IP 주소, 넷마스크, 호스트 이름 및 기본 게이트웨이를 유지하려면 액세스 포인트를 LWAPP로 전환하기 전에 액세스 포인트에 이러한 자동 이미지 중 하나를 로드해야 합니다 .12.3(7)JA12.3(7)JA112.3(7)JA212.3(7)JA312.3(7)JA412.3(8)JA12.3(8)JA112.3(8)JA212.3(8)JEA12.3(8)JEA112.3(8)JEA212.3(8)JEB12.3(8)JEB112.4(3g) JA12.4(3g) JA1
- 이러한 자율 이미지 중 하나에서 액세스 포인트를 LWAPP로 업그레이드할 경우 변환된 액세스 포인트는 고정 IP 주소, 넷마스크, 호스트 이름 및 기본 게이트웨이를 유지하지 않습니다

.12.3(11)JA12.3(11)JA112.3(11)JA212.3(11)JA3
- 업그레이드 프로세스가 완료되면 LWAPP 업그레이드 도구는 Windows 운영 체제 메모리 리소스를 릴리스하지 않습니다.메모리 리소스는 업그레이드 도구를 종료한 후에만 해제됩니다.여러 액세스 포인트 배치를 업그레이드할 경우 메모리 리소스를 릴리스하려면 배치 사이에 도구를 종료해야 합니다.일괄 처리 사이에 도구를 종료하지 않으면 과도한 메모리 소비로 인해 업그레이드 스테이션의 성능이 빠르게 저하됩니다.

인증서 유형

AP에는 두 가지 종류가 있습니다.

- MIC가 있는 AP
- SSC가 필요한 AP

출하 시 설치된 인증서는 Manufacturing Installed Certificate의 약어인 MIC에서 참조합니다.2005년 7월 18일 이전에 출시된 Cisco Aironet 액세스 포인트에는 MIC가 없으므로, 이러한 액세스 포인트는 경량형 모드에서 작동하도록 업그레이드될 때 자체 서명 인증서를 생성합니다.컨트롤러는 특정 액세스 포인트 인증을 위해 자체 서명 인증서를 허용하도록 프로그래밍됩니다.

Aironet 1000 AP와 같이 LWAPP(Lightweight Access Point Protocol)를 사용하는 Cisco Aironet MIC AP를 처리하고 그에 따라 문제를 해결해야 합니다.즉, IP 연결을 확인하고 LWAPP 상태 시스템을 디버깅한 다음 crypto를 확인합니다.

업그레이드 도구 로그는 AP가 MIC AP인지 SSC AP인지 보여줍니다.다음은 업그레이드 툴의 자세한 로그 예입니다.

```
2006/08/21 16:59:07 INFO  172.16.1.60  Term Length configured.
2006/08/21 16:59:07 INFO  172.16.1.60  Upgrade Tool supported AP
2006/08/21 16:59:07 INFO  172.16.1.60  AP has two radios
2006/08/21 16:59:07 INFO  172.16.1.60  AP has Supported Radio
2006/08/21 16:59:07 INFO  172.16.1.60  AP  has 12.3(7)JA Image or greater
2006/08/21 16:59:07 INFO  172.16.1.60  Station role is  Root AP
2006/08/21 16:59:07 INFO  172.16.1.60  MIC is already configured in the AP
2006/08/21 16:59:07 INFO  172.16.1.60      Hardware is PowerPC405GP Ethernet,
                                         address is 0015.63e5.0c7e (bia 0015.63e5.0c7e)
2006/08/21 16:59:08 INFO  172.16.1.60  Inside Shutdown function
2006/08/21 16:59:10 INFO  172.16.1.60  Shutdown the Dot11Radio1
2006/08/21 16:59:11 INFO  172.16.1.60  Shutdown the Dot11Radio0
2006/08/21 16:59:12 INFO  172.16.1.60  Updating the AP with Current System Time
2006/08/21 16:59:13 INFO  172.16.1.60  Saving the configuration into memory
2006/08/21 16:59:13 INFO  172.16.1.60  Getting  AP Name
2006/08/21 16:59:58 INFO  172.16.1.60  Successfully Loaded the LWAPP Recovery
                                         Image on to the AP
2006/08/21 16:59:58 INFO  172.16.1.60  Executing Write Erase Command
2006/08/21 17:00:04 INFO  172.16.1.60  Flash contents are logged
2006/08/21 17:00:06 INFO  172.16.1.60  Environmental Variables are logged
2006/08/21 17:00:06 INFO  172.16.1.60  Reloading the AP
2006/08/21 17:00:08 INFO  172.16.1.60  Successfully executed the Reload command
```

이 로그에서 강조 표시된 줄은 AP에 MIC가 설치되어 있음을 나타냅니다.인증서 및 업그레이드 프로세스에 대한 자세한 내용은 자동 Cisco Aironet 액세스 포인트를 경량 모드로 업그레이드의 업그레이드 프로세스 개요 섹션을 참조하십시오.

SSC AP의 경우 컨트롤러에 인증서가 생성되지 않습니다.업그레이드 툴에는 AP에서 자체 생성 인증서(SSC)에 서명하는 데 사용되는 Rivest, Shamir 및 Adelman(RSA) 키 쌍을 생성합니다. 업그레

이드 툴은 AP의 MAC 주소 및 공개 키 해시의 컨트롤러 인증 목록에 항목을 추가합니다.SSC 서명을 검증하려면 컨트롤러에서 공개 키 해시가 필요합니다.

항목이 컨트롤러에 추가되지 않은 경우 출력 CSV 파일을 확인합니다.각 AP에 대한 항목이 있어야 합니다.항목을 찾으면 해당 파일을 컨트롤러로 가져옵니다.컨트롤러 CLI(Command-Line Interface)(**config auth-list** 명령 사용) 또는 스위치 웹을 사용하는 경우 한 번에 하나의 파일을 가져와야 합니다.WCS를 사용하면 전체 CSV 파일을 템플릿으로 가져올 수 있습니다.

또한 규정 도메인을 확인합니다.

참고:LAP AP가 있지만 Cisco IOS 기능을 사용하려면 자율 Cisco IOS 이미지를 로드해야 합니다.반대로 자동 AP가 있고 이를 LWAPP로 변환하려는 경우 자동 IOS를 통해 LWAPP 복구 이미지를 설치할 수 있습니다.

MODE 버튼 또는 CLI **아카이브 다운로드** 명령을 사용하여 AP 이미지를 변경하는 단계를 완료할 수 있습니다.AP 모델 기본 파일 이름으로 명명된 자동 IOS 또는 복구 이미지와 작동하는 MODE 버튼 이미지 다시 로드를 사용하는 방법에 대한 자세한 내용은 문제 해결을 참조하십시오.

다음 섹션에서는 업그레이드 작업에서 일반적으로 나타나는 몇 가지 문제 및 이러한 문제를 해결하는 단계에 대해 설명합니다.

문제

증상

AP가 컨트롤러에 조인하지 않습니다.이 문서의 Solutions(솔루션) 섹션에서는 확률 순서로 원인을 제공합니다.

솔루션

이 섹션을 사용하여 이 문제를 해결하십시오.

원인 1

AP가 LWAPP 검색을 통해 컨트롤러를 찾을 수 없거나 AP가 컨트롤러에 연결할 수 없습니다.

문제 해결

다음 단계를 완료하십시오.

1. 컨트롤러 CLI에서 **debug lwapp events enable** 명령을 실행합니다.LWAPP 검색 > 검색 응답 > 조인 요청 > 조인 응답 시퀀스를 찾습니다.LWAPP 검색 요청이 표시되지 않으면 AP에서 컨트롤러를 찾을 수 없거나 찾을 수 없음을 의미합니다.다음은 WLC(Wireless LAN Controller)에서 변환된 LAP(Lightweight AP)로의 성공적인 JOIN REPLY의 예입니다. 다음은 debug lwapp **events enable** 명령의 출력입니다.

```
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP
                          00:15:63:e5:0c:7e to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
                          00:15:63:e5:0c:7e on Port 1
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
```

```
                          to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to AP
                          00:15:63:e5:0c:7e on Port 1
Thu May 25 06:53:54 2006: Received LWAPP DISCOVERY REQUEST from AP 00:15:63:e5:0c:7e
                          to ff:ff:ff:ff:ff:ff on port '1'
Thu May 25 06:53:54 2006: Successful transmission of LWAPP Discovery-Response to
                          AP 00:15:63:e5:0c:7e on Port 1
Thu May 25 06:54:05 2006: Received LWAPP JOIN REQUEST from AP 00:15:63:e5:0c:7e
                          to 00:0b:85:33:84:a0 on port '1'
Thu May 25 06:54:05 2006: LWAPP Join-Request MTU path from AP 00:15:63:e5:0c:7e
                          is 1500, remote debug mode is 0
Thu May 25 06:54:05 2006: Successfully added NPU Entry for AP 00:15:63:e5:0c:7e
                          (index 51)Switch IP: 172.16.1.11, Switch Port: 12223,
                          intIfNum 1, vlanId 0AP IP: 172.16.1.60, AP Port: 20679,
                          next hop MAC: 00:15:63:e5:0c:7e
Thu May 25 06:54:05 2006: Successfully transmission of LWAPP Join-Reply to AP
                          00:15:63:e5:0c:7e
.......................................
.......................................
..................................... // the debug output continues for
full registration process.
```

2. AP 네트워크와 컨트롤러 간의 IP 연결을 확인합니다.컨트롤러와 AP가 동일한 서브넷에 있는 경우 올바르게 상호 연결되어 있는지 확인합니다.서로 다른 서브넷에 있는 경우 라우터가 두 서브넷 간에 사용되고 두 서브넷 간에 라우팅이 제대로 활성화되어 있는지 확인합니다.
3. 검색 메커니즘이 올바르게 구성되었는지 확인합니다.DNS(Domain Name System) 옵션을 사용하여 WLC를 검색하는 경우 DNS 서버가 WLC IP 주소와 CISCO-LWAPP-CONTROLLER.local-domain을 매핑하도록 올바르게 구성되었는지 확인합니다.따라서 AP에서 이름을 확인할 수 있는 경우 확인된 IP 주소에 LWAPP 가입 메시지를 발행합니다.옵션 43을 검색 옵션으로 사용하는 경우 DHCP 서버에 제대로 구성되었는지 확인합니다.검색 프로세스 및 시퀀스에 대한 자세한 내용은 WLC에 LAP 등록을 참조하십시오.DHCP 옵션 43을 구성하는 방법에 대한 자세한 내용은 DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example을 참조하십시오.**참고:** 고정으로 주소가 지정된 AP를 변환할 때 고정 주소가 업그레이드 중에 유지되므로 작동하는 유일한 레이어 3 검색 메커니즘은 DNS입니다.AP에서 정확한 발생을 확인하기 위한 충분한 정보를 수신하기 위해 debug lwapp **client events** 명령 및 **debug ip udp** 명령을 실행할 수 있습니다.다음과 같은 UDP(User Datagram Protocol) 패킷 시퀀스가 표시되어야 합니다.컨트롤러 관리 인터페이스 IP를 사용하여 AP IP에서 제공컨트롤러 AP 관리자 IP에서 AP IP로 소스AP IP에서 AP 관리자 IP로 소싱되는 일련의 패킷입니다.**참고:** 경우에 따라 여러 컨트롤러가 있을 수 있으며 AP가 LWAPP 검색 상태 시스템 및 알고리즘을 기반으로 다른 컨트롤러에 조인하려고 시도할 수도 있습니다.이 상황은 컨트롤러가 수행하는 기본 동적 AP 로드 밸런싱 때문에 발생할 수 있습니다.이 상황은 검토할 가치가 있다.**참고:** 다음은 debug **ip udp** 명령의 예제 출력입니다.

```
Dec 16 00:32:08.228: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12222),
                     length=78
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=60
*Dec 16 00:32:08.777: UDP: sent src=172.16.1.60(20679), dst=172.16.1.10(12223),
                     length=75
*Dec 16 00:32:08.778: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:08.779: UDP: rcvd src=172.16.1.10(12223), dst=172.16.1.60(20679),
                     length=59
*Dec 16 00:32:09.057: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=180
*Dec 16 00:32:09.059: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                     length=22
*Dec 16 00:32:09.075: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                     length=89
```

```
*Dec 16 00:32:09.077: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                      length=22
*Dec 16 00:32:09.298: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                      length=209
*Dec 16 00:32:09.300: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                      length=22
*Dec 16 00:32:09.300: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                      length=164
*Dec 16 00:32:09.301: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                      length=22
*Dec 16 00:32:09.302: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                      length=209
*Dec 16 00:32:09.303: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                      length=22
*Dec 16 00:32:09.303: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                      length=287
*Dec 16 00:32:09.306: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                      length=22
*Dec 16 00:32:09.306: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                      length=89
*Dec 16 00:32:09.308: UDP: rcvd src=172.16.1.11(12223), dst=172.16.1.60(20679),
                      length=22
*Dec 16 00:32:09.308: UDP: sent src=172.16.1.60(20679), dst=172.16.1.11(12223),
                      length=222
```

해결

다음 단계를 완료하십시오.

1. 설명서를 검토합니다.
2. LWAPP 검색을 올바르게 지원하도록 인프라를 수정하십시오.
3. AP를 프라임 레이션하기 위해 컨트롤러와 동일한 서브넷으로 이동합니다.
4. 필요한 경우 AP CLI에서 **컨트롤러 IP를 수동으로 설정하려면 lwapp ap controller ip address *A.B.C.D* 명령**을 실행합니다.이 명령의 *A.B.C.D* 부분은 WLC의 관리 인터페이스 IP 주소입니다.**참고:** 이 CLI 명령은 컨트롤러에 등록하지 않은 AP나 이전 컨트롤러에 조인된 동안 기본 enable 비밀번호가 변경된 AP에서 사용할 수 있습니다.자세한 내용은 경량 AP(LAP)에서 LWAPP 컨피그레이션 재설정을 참조하십시오.

원인 2

컨트롤러 시간이 인증서 유효 기간을 벗어났습니다.

문제 해결

다음 단계를 완료하십시오.

1. debug lwapp **오류 enable** 및 debug pm pki enable 명령**을** 실행합니다.이러한 **debug** 명령은 AP와 WLC 간에 전달되는 인증서 메시지의 디버그를 표시합니다.이 명령은 인증서가 유효 기간을 벗어난 것으로 거부된다는 메시지를 분명히 보여줍니다.**참고:** UTC(Coordinated Universal Time) 오프셋을 고려해야 합니다.컨트롤러의 debug pm pki enable 명령**의** 출력입니다.

```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
```

```
                          L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e,
                          MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer>  O=Cisco Systems,
                          CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
                          00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems.
.......................
.......................
.......................
.......................
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using
                          >cscoDefaultMfgCaCert<
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
                          2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert
                          validity interval: make sure the controller time is set.
Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil)
```

이 출력에서 강조 표시된 정보를 확인합니다.이 정보는 **컨트롤러 시간**이 **AP의 인증서 유효 기간을 벗어났음을** 분명히 보여줍니다.따라서 AP는 컨트롤러에 등록할 수 없습니다.AP에 설치된 인증서에는 사전 정의된 유효성 간격이 있습니다.컨트롤러 시간은 AP의 인증서 유효 간격 내에 있는 방식으로 설정해야 합니다.

2. AP에서 설정된 인증서 유효성 간격을 확인하기 위해 AP CLI에서 **show crypto ca certificates** 명령을 실행합니다.예:

```
AP0015.63e5.0c7e#show crypto ca certificates
.........................................
.........................................
.........................................
.........................................
Certificate
  Status: Available
  Certificate Serial Number: 4BC6DAB80000000517AF
  Certificate Usage: General Purpose
  Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
  Subject:
    Name: C1200-001563e50c7e
    ea=support@cisco.com
    cn=C1200-001563e50c7e
    o=Cisco Systems
    l=San Jose
    st=California
    c=US
  CRL Distribution Point:
    http://www.cisco.com/security/pki/crl/cmca.crl
  Validity Date:
    start date: 17:22:04 UTC Nov 30 2005
    end   date: 17:32:04 UTC Nov 30 2015
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: Cisco_IOS_MIC_cert
.................................
.................................
.................................
```

이 명령의 출력과 관련된 여러 유효성 간격이 있을 수 있으므로 전체 출력이 나열되지 않습니다.연결된 신뢰 지점에서 지정한 유효성 간격만 고려해야 **합니다.**이름 필드에 관련 AP 이름이 있는 **Cisco_IOS_MIC_cert**(**여기, 이름:C1200-001563e50c7e**)는 이 출력 예에서 강조 표시되어 있습니다.**고려할 실제 인증서 유효 간격입니다.**

3. 컨트롤러 CLI에서 **show time** 명령을 실행하여 컨트롤러에서 설정한 날짜와 시간이 이 유효성

간격 내에 있는지 확인합니다.컨트롤러 시간이 이 인증서 유효 간격보다 높거나 낮으면 컨트롤러 시간을 이 간격 이내로 변경합니다.

해결

이 단계를 완료합니다.

컨트롤러 **GUI** 모드에서 Commands > Set Time을 선택하거나 컨트롤러 CLI에서 **config time** 명령을 실행하여 컨트롤러 시간을 설정합니다.

원인 3

SSC AP에서는 SSC AP 정책을 사용할 수 없습니다.

문제 해결

이러한 경우 컨트롤러에서 다음 오류 메시지가 표시됩니다.

```
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 1553: spamProcessJoinRequest
                          :spamDecodeJoinReq failed
Wed Aug  9 17:20:21 2006  [ERROR] spam_crypto.c 1509: Unable to free public key for
                          AP 00:12:44:B3:E5:60
Wed Aug  9 17:20:21 2006  [ERROR] spam_lrad.c 4880: LWAPP Join-Request does not include
                          valid certificate in CERTIFICATE_PAYLOAD from
                          AP 00:12:44:b3:e5:60.
Wed Aug  9 17:20:21 2006  [CRITICAL] sshpmPkiApi.c 1493: Not configured to accept
                          Self-signed AP cert
```

다음 단계를 완료하십시오.

다음 두 작업 중 하나를 수행합니다.

- 컨트롤러 CLI에서 **show auth-list** 명령을 실행하여 컨트롤러가 SSC가 있는 AP를 허용하도록 구성되었는지 확인합니다.다음은 **show auth-list** 명령의 샘플 출력입니다.
  ```
  #show auth-list


  Authorize APs against AAA ..... disabled

  Allow APs with Self-signed Certificate (SSC) .... enabled


  Mac Addr                  Cert Type    Key Hash

  ----------------------    ----------   ----------------------------------------

  00:09:12:2a:2b:2c         SSC          12345678901234567890123456789012345678901
  ```
- GUI에서 **Security(보안) > AP Policies(AP 정책)**를 선택합니다.

1. Accept **Self Signed Certificate** 확인란이 활성화되었는지 확인합니다.그렇지 않으면 활성화합니다.
2. SSC를 인증서 유형으로 선택합니다.

3. MAC 주소 및 키 해시를 사용하여 권한 부여 목록에 AP를 추가합니다.이 키 해시는 debug pm pki enable 명령의 출력에서 가져올 수 있습니다.key-hash 값을 가져오는 방법은 원인 4를 참조하십시오.

원인 4

SSC 공개 키 해시가 잘못되었거나 없습니다.

문제 해결

다음 단계를 완료하십시오.

1. debug lwapp **events enable** 명령을 실행합니다.AP가 참가를 시도하는지 확인합니다.
2. show auth-**list** 명령을 실행합니다.이 명령은 컨트롤러에서 스토리지에 있는 공개 키 해시를 표시합니다.
3. debug pm pki enable 명령을 실행합니다.이 명령은 실제 공개 키 해시를 표시합니다.실제 공개 키 해시는 컨트롤러에서 스토리지에 있는 공개 키 해시와 일치해야 합니다.불일치로 인해 문제가 발생합니다.이 디버그 메시지의 샘플 출력입니다.

```
(Cisco Controller) > debug pm pki enable

Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle...
Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert>
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert
>bsnDefaultRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert
>bsnDefaultCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert
>bsnDefaultBuildCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert
>cscoDefaultNewRootCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert
>cscoDefaultMfgCaCert<
Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert
>bsnOldDefaultIdCert<
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key
Data
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  30820122 300d0609
2a864886 f70d0101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  01050003 82010f00
3082010a 02820101
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  00c805cd 7d406ea0
cad8df69 b366fd4c
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  82fc0df0 39f2bff7
ad425fa7 face8f15
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f356a6b3 9b876251
43b95a34 49292e11
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  038181eb 058c782e
56f0ad91 2d61a389
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  f81fa6ce cd1f400b
b5cf7cef 06ba4375
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  dde0648e c4d63259
774ce74e 9e2fde19
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  0f463f9e c77b79ea
65d8639b d63aa0e3
Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data  7dd485db 251e2e07
9cd31041 b0734a55
```

```
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  463fbacc 1a61502d
c54e75f2 6d28fc6b
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  82315490 881e3e31
02d37140 7c9c865a
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  9ef3311b d514795f
7a9bac00 d13ff85f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  97e1a693 f9f6c5cb
88053e8b 7fae6d67
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  ca364f6f 76cf78bc
bc1acc13 0d334aa6
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  031fb2a3 b5e572df
2c831e7e f765b7e5
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  fe64641f de2a6fe3
23311756 8302b8b8
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  1bfae1a8 eb076940
280cbed1 49b2d50f
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data  f7020301 0001
Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: SSC Key Hash is
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This is the actual SSC key-hash value. Mon May 22 06:34:14 2006: LWAPP Join-Request
MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode is 0 Mon May 22 06:34:14
2006: spamRadiusProcessResponse: AP Authorization failure for
00:0e:84:32:04:f0
```

해결

다음 단계를 완료하십시오.

1. debug pm pki enable 명령 출력에서 public key-hash를 **복사하고** 이를 사용하여 인증 목록에서 public key-hash를 대체합니다.
2. AP **MAC** 주소 및 키 해시를 권한 부여 목록에 추가하려면 config auth-list add ssc *AP_MAC AP_key* ***명령***을 실행합니다.다음은 이 명령의 예입니다.

```
(Cisco Controller)>config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

원인 5

AP에 인증서 또는 공개 키 손상이 있습니다.

문제 해결

이 단계를 완료합니다.

debug lwapp **오류 enable** 및 debug pm pki enable 명령**을** 실행합니다.

손상된 인증서 또는 키를 나타내는 메시지가 표시됩니다.

해결

다음 두 옵션 중 하나를 사용하여 문제를 해결합니다.

- MIC AP - RMA(Return Materials Authorization)를 요청합니다.

- SSC AP - Cisco IOS Software 릴리스 12.3(7)JA로 다운그레이드합니다.다운그레이드하려면 다음 단계를 완료하십시오.

1. 재설정 버튼 옵션을 사용합니다.
2. 컨트롤러 설정을 지웁니다.
3. 업그레이드를 다시 실행합니다.

원인 6

컨트롤러가 레이어 2 모드에서 작동할 수 있습니다.

문제 해결

이 단계를 완료합니다.

컨트롤러의 작동 모드를 확인합니다.

변환된 AP는 레이어 3 검색만 지원합니다.변환된 AP는 레이어 2 검색을 지원하지 않습니다.

해결

다음 단계를 완료하십시오.

1. WLC를 레이어 3 모드로 설정합니다.
2. 재부팅하고 AP 관리자 인터페이스에 관리 인터페이스와 동일한 서브넷의 IP 주소를 지정합니다.서비스 포트(예: 4402 또는 4404의 서비스 포트)가 있는 경우 AP 관리자 및 관리 인터페이스와 다른 수퍼넷에 있어야 합니다.

원인 7

업그레이드하는 동안 다음 오류가 표시됩니다.

```
FAILED   Unable to Load  the LWAPP Recovery Image on to the AP
```

문제 해결

이 오류가 표시되면 다음 단계를 완료합니다.

1. TFTP 서버가 올바르게 구성되었는지 확인합니다.Upgrade Tool 내장 TFTP 서버를 사용하는 경우, 일반적인 원인은 수신 TFTP를 차단하는 개인 방화벽 소프트웨어입니다.
2. 업그레이드에 올바른 이미지를 사용하고 있는지 확인합니다.경량 모드로 업그레이드하려면 특수 이미지가 필요하며 일반 업그레이드 이미지로는 작동하지 않습니다.

원인 8

변환 후 AP에서 다음 오류 메시지가 표시됩니다.

```
*Mar 1 00:00:23.535: %LWAPP-5-CHANGED: LWAPP changed state to DISCOVERY
```

```
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_
                     certs no certs in the SSC Private File
*Mar 1 00:00:23.550: LWAPP_CLIENT_ERROR_DEBUG:
*Mar 1 00:00:23.551: lwapp_crypto_init: PKI_StartSession failed
*Mar 1 00:00:23.720: %SYS-5-RELOAD: Reload requested by LWAPP CLIENT.
                     Reload Reason: FAILED CRYPTO INIT.
*Mar 1 00:00:23.721: %LWAPP-5-CHANGED: LWAPP changed state to DOWN
```

30초 후에 AP가 다시 로드되고 프로세스가 다시 시작됩니다.

해결

이 단계를 완료합니다.

SSC AP가 있습니다.LWAPP AP로 변환한 후 컨트롤러의 AP Authentication(AP 인증) 목록 아래에 SSC 및 MAC 주소를 추가합니다.

문제 해결 팁

다음 팁은 자율 모드에서 LWAPP 모드로 업그레이드할 때 사용할 수 있습니다.

- 변환 후 컨트롤러에서 쓰기 작업을 시도할 때 NVRAM이 지워지지 않으면 문제가 발생합니다.AP를 LWAPP로 변환하기 전에 컨피그레이션을 지우는 것이 좋습니다.컨피그레이션을 지우려면IOS GUI에서 System **Software(시스템 소프트웨어) > System Configuration(시스템 컨피그레이션) > Reset to Defaults(기본값으로 재설정)** 또는 **Reset to Defaults Except IP(IP를 제외한 기본값으로 재설정)로 이동합니다**.CLI에서 - CLI에서 **write erase** 및 **reload** 명령을 실행하며 프롬프트가 표시되면 컨피그레이션을 저장할 수 없습니다.이렇게 하면 AP의 텍스트 파일이 업그레이드 툴에서 변환되어 항목이 <ip address>,Cisco,Cisco,Cisco가 되면서 간단하게 만들 수 있습니다.
- tftp32를 사용하는 것이 좋습니다. 최신 TFTPD 서버는 http://tftpd32.jounin.net/에서 다운로드할 수 있습니다 .
- 업그레이드 프로세스 중에 방화벽 또는 액세스 제어 목록이 활성화된 경우 업그레이드 툴은 환경 변수가 포함된 파일을 워크스테이션에서 AP로 복사할 수 없습니다.방화벽 또는 액세스 제어 목록이 복사 작업을 차단하고 Use Upgrade Tool TFTP Server 옵션을 선택하는 경우, 도구가 환경 변수를 업데이트할 수 없고 AP에 이미지 업로드가 실패하므로 업그레이드를 진행할 수 없습니다.
- 업그레이드하려는 이미지를 다시 확인하십시오.IOS에서 LWAPP 이미지로 업그레이드하는 작업은 일반 IOS 이미지와 다릅니다.내 문서/내 컴퓨터—> 도구—> 폴더 옵션에서 **알려진 파일 형식에 대해 파일 확장명 숨기기** 확인란**의 선택을** 취소해야 합니다.
- 항상 사용 가능한 최신 업그레이드 도구 및 업그레이드 복구 이미지를 사용해야 합니다.최신 버전은 무선 소프트웨어 센터에서 사용할 수 있습니다.
- AP는 **.tar** 이미지 파일을 부팅할 수 없습니다.zip 파일과 유사한 아카이브 파일입니다.**archive download** 명령을 사용하여 **.tar** 파일을 AP 플래시로 **번들링하지** 않거나 tar 파일에서 부트 가능한 이미지를 가져온 다음 부트 가능한 이미지를 AP 플래시에 넣어야 합니다.

관련 정보

- 자동 Cisco Aironet 액세스 포인트를 경량 모드로 업그레이드
- 경량 AP(LAP)에서 LWAPP 컨피그레이션 재설정
- DHCP OPTION 43 for Lightweight Cisco Aironet Access Points 컨피그레이션 예

- 액세스 포인트의 해시 키를 복구하여 컨트롤러로 가져오는 방법
- CLI를 사용하여 Cisco Aironet 자동 액세스 포인트를 LWAPP(Lightweight Access Point Protocol)로 변환할 수 있습니까?
- 기술 지원 및 문서 – Cisco Systems